Office of Information Technology
Five Year Plan

Contents

The Public Sector Challenge

McKinsey Insights, 12/ 2014 --

Digital transformations require changes, to both processes and IT systems that are more challenging to implement in the public sector than in the private sector. A joint study by McKinsey and Oxford University found that public-sector IT projects requiring business change were six times more likely to experience cost overruns and 20 percent more likely to run over schedule than such projects in the private sector.

The public sector must cope with additional management issues, including multiple agencies, a range of organizational mandates and constituencies, longer appropriations timelines, and the challenge of maintaining strategic continuity even as political administrations change.

Therefore, it is important that private-sector companies supporting public IT transformations understand that the public sector operates in a different context. For example, it can be challenging to set a specific target, build consensus, align on a leadership structure, secure funding, and meet implementation timelines.

Similarly, when systems and data are owned by different departments and functions, on a range of platforms and with differing taxonomies and access requirements, it can be difficult to invest at scale and generate sufficient economies. Silos, fragmentation, and the absence of a central owner for nationwide IT infrastructure and common components can make it hard to connect the internal "plumbing" to create a seamless experience for the end user, be it a government worker, a business user, an average citizen, or another intergovernmental office. It doesn't make the task easier when the complexity of large-scale digital projects requires specialized skills and expertise that come at a high price and are often in short supply. In consequence, many e-government efforts fall short of their promise.

Public CIO Magazine, November 2014, pg. 11 --

When there is not a governance model supporting shared services, agencies that have the funding will often spend dollars on separate, siloed systems instead of pooling their budgets and purchasing a single system they're able to maintain and manage over time. These siloed systems often require more resources than an agency has to sustain. Tax dollars are wasted on duplicative technologies and freestanding applications, and it's more expensive and time consuming to operate, manage and maintain legacy infrastructure.

Maine's Foundation for the Future

The State of Maine's Office of Information Technology's five year strategy will encompass project delivery, building a resilient, redundant, and flexible infrastructure, and risk management (cyber security and disaster recovery). The foundation will be:

1. **Business Process Management** (BPM) for process efficiency
2. **Agile Methodology** for predicable project delivery
3. **Enterprise Strategy** for reusable systems.
4. **Workforce Development** for finding, training the needed resources

Executive Summary

The demand for responsive, efficient, mobile digital government services is increasing exponentially; we must evolve the OIT organization to meet this demand.

The Challenge: Meeting the demand for services

Agencies and OIT are already struggling to meet citizen demand with aging and brittle applications running on infrastructure that was designed – over 15 years ago -- for a static and siloed world. And citizen expectations have evolved: business and private citizens want to do business with one state of Maine, not 14 separate entities.

OIT current challenges include:

- Ever changing cyber security threats
- Digital Government Services Delivery to business and private constituents
- Transparent data sharing and analytics
- The pace of policy, new legislation, and federal mandates
- Customer services levels measured in hours not weeks and months
- Pressure on Program and Technology Budgets

The Evolved Approach: Enterprise Modernization

OIT proposes over the next five years to develop a focused strategy of enterprise modernization:

Business Process Management	Agile Delivery	Legacy Modernization	Risk Management	Workforce Development
- Help Agencies to respond to changes quickly - Empower Agencies to make changes themselves - Reuse tools that work across government - New tools and products quicker to market	- Agencies drive the priorities - Agenices control costs - Implementations are 3 times more successful - Making changes is low risk and straight forward - Predictibile project delivery	- Methodically retire expensive legacy systems - Replace aging inflexible hardware - Develop a modern flexible workforce - Currenly legacy maintenance is costing $25M in FTE support annually	- Redesign aging, vunerable networks - Design infrastructure with disaster recover included - Bolster our cyber security workforce and tools	- Hire to new skills and talent -Harmonize skills around small number of platforms and technologies - Knowledge transfer to new workforce - Address shrinking talent pool through interns and outreach

Enterprise Strategy

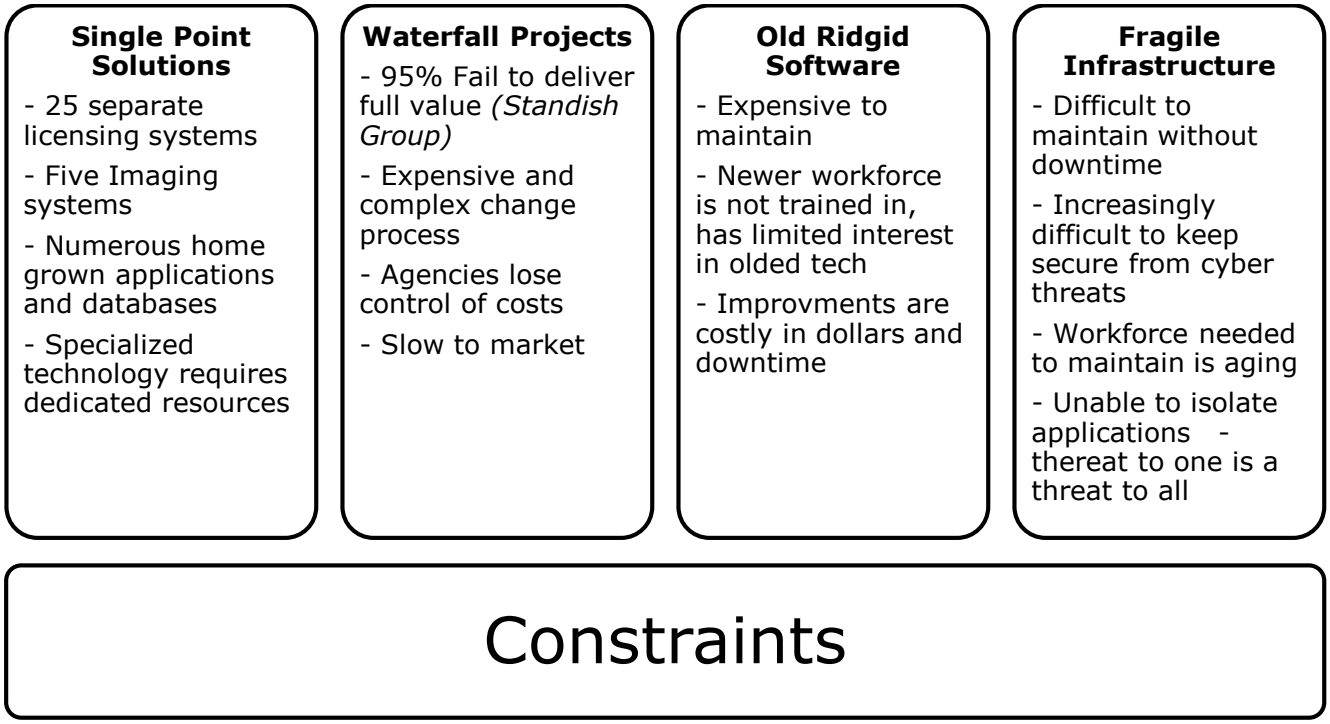
Investment in these five strategic areas will result in reduced development costs, reusability of assets, predicable delivery, and flexibility.

Constraints

Since the technology consolidation in 2005, we have made great strides in centralizing client and infrastructure services. This has resulted in more stable, secure and lower cost services to agencies; and the State IT workforce has 80 less FTEs than before the consolidation. But over time, with the pressure to continually lower costs we have deferred investment in the infrastructure. This lack of investment has resulted in a less flexible, higher cost, higher risk environment.

The Office of Information Technology maintains an inventory of over 600 applications, many built on outdated technologies. Refreshing applications or migrating to newer, modern, and flexible platforms requires time and money, and involves risk (change) to the Agencies.

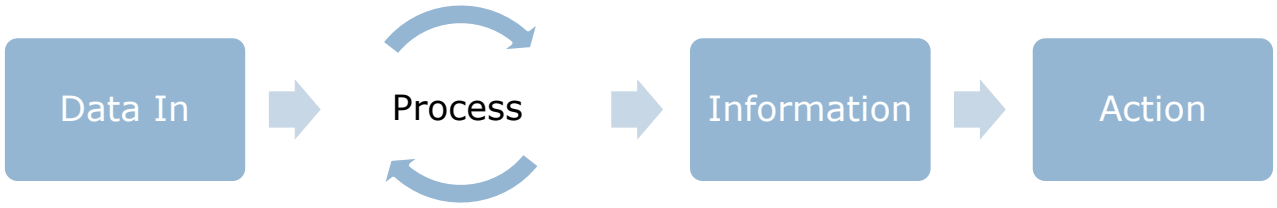
Additionally, agencies have often invested in single point solutions (multiple imaging systems, licensing systems, etc.) instead of enterprise solutions. This is often driven by the timing of Federal funding, but has resulted in a hodge-podge of expensive boutique solutions. Multiple solutions, with multiple technologies, require more, expensive resources to maintain them – reducing economies of scale.



We need to evolve the world of legacy applications and infrastructure, and agency-specific applications, to a world of Enterprise strategy and vision, modern tools and methodology, and predictable delivery. We need to evolve from a world where we are building applications many times and using once, to a world where we building once and use many – true shared services.

1 - Business Process Management for Operational Efficiency

Business Process Management (BPM) is the technology and discipline to build systems based on the most efficient way to process work. Almost everything we do in the State of Maine involves process:



Today's mix of manual processes and legacy applications has left an expensive (FTEs) and unsustainable system. BPM is a way to untangle the pipes – to straighten the flow.

Immediately deliver operational efficiencies

Business Process Management has been embraced by the private sector for more than ten years as a way to drive efficiency and improve service delivery. Gartner studies have listed business process management as the *primary driver of operational efficiency* since 2009, ahead of legacy modernization.

The value of Business Process Management is well documented. When an organization modernizes their systems and processes with a mature BPM application they see a 20% reduction in maintenance costs, 30% reduction in operational costs, and a 20% reduction in new employee onboarding time.

Coordinate and reuse applications

Business Process Management builds applications based on how people do work, their processes. These processes may be broken down into reusable "modules" of functionality. For instance, almost any application used by the public requires the creation of an account and login. We have now built this process called, "Manage Account" through BPM. The first time the module was built, the development effort was two weeks, when it was subsequently reused, it took two days to configure and brand the login screens.

As we continue to develop applications in BPM, we are building a library of modules that are being reused across seemingly unrelated Agencies and applications. Some items created to date include a module to accept electronic payments directly from citizens, and a portal to login and create an account. By building once and reusing many times we are both making applications consistent across the State as well as saving money and time.

Accounts Payable	Blocked Claims	Fisheries Licensing and Information	Pesticides Licensing
Approvals	Audit	Apply for License	Certification
Authorization	Create case	Create account	Create account
Cash and Allotment	ECM	Data collection	Eligibility Tracking
Disbursement approval	Field Audit	Enforcement	Enforcement
Intake	Intake	Entity Search	Entity Search
Integration	Integration	Grant license	Inspections
Internal Controls	Management Approval	Integration	Licensing
Invoicing	Update case	Landing page	Manage account
Reporting		Licensing	Notification
Routing		Manage account	Payments
Travel		Payments	Registrations
Validate Chart of Accounts			Renewal
Validation			Reporting
			Request Assistance

Current BPM reusable modules

Improve Constituent (Customer) Perception

One of the most important aspects of a BPM application is improved internal and external customer perception. Users of the application are provided an easy to understand user interface requiring little training as well as automatic notifications. The user experience is meant to be similar to that found on Amazon.com or TurboTax. One does not need to take training to order items from Amazon this is the direction for our BPM applications as well.

Forty Hour Applications

OIT has partnered with various Agencies in rapid development of BPM applications as part of a new program call Forty Hour Apps. An Agency partner identifies a paper intensive process often convoluted and difficult to manage.

A single developer is paired with an Agency subject matter expert to redefine the process and make it electronic. Over the course of 40 hours, the developer and subject matter expert build an application that replaces the legacy process. The resulting application focuses on automating and making transparent the old process. Finally, any changes to the application may be made by Agency personnel so assistance from OIT or contracted developers is minimized.

Some examples of Forty Hour Apps include: Out of State Travel Request approval, FJA Tracking, and Exemption to Hire Position.

The focus on Forty Hour Apps will only increase over the coming quarters as we find and optimize many of these self-imposed, paper based problems. A well regarded IBM study found that an electronic copy of a paper process is automatically 12% more efficient. BPM further optimizes the work so returns should be in excess of this amount.

1.1 - Potential Operational Improvements - BPM in action

Operational Efficiencies

A mature organization following strict business process management methodologies is able to achieve 10 - 20% savings in operational workforce

A State of Maine model for this can be seen over the past eight years at Maine Revenue Services where, through automation, they reduced the workforce by more than 70 FTEs saving $1.1M annually, net of infrastructure and automation investments.

If we take a conservative estimate of even 5% savings, we could reduce the DAFS workforce by more than 68 FTEs representing cost savings of approximately $6M annually.

OIT Billing

OIT is continually looking to improve the way we bill and help agencies budget for IT. Billing and budgeting are intertwined in that the more accurate the billing, the better that information can be used to inform a major component of the IT budget process. Improving both involve collaborative participation of Agency, Service Center, Bureau of Budget, and OIT personnel.

In addition to continued efforts on the budget process, OIT is embarking on a full review and documentation of OIT Billing. We are working with the OIT Project Management Office and the BPM center of excellence and will utilize business process management to ensure that the billing system is as accurate and efficient as possible while meeting the various needs of our business partners.

The end goal of the OIT Billing project is to have accurate, complete, and transparent billing of all OIT services in a way customers can trust and understand. In addition to customer satisfaction, billing that is accurate and complete means that customers feel comfortable with paying their invoice and using that information to help inform their budgetary needs, and OIT feels comfortable that we are billing and then receiving the appropriate amounts to cover our costs.

Specifically, we will document every billing stream, understand the source data, flow it through the billing process and how the customer sees the information, tie it to how it is described in the OIT Service Catalog, tie it to what we've posted for rates, etc. This will identify current processes and highlight concerns (such as the fact that you can't

currently tie an Application Budget – ie $1MM for ACES – to the details of billing) as well as point out major gaps.

Documenting the process, understanding the gaps, and learning other details as we work through the project will help us:

- Fix "low hanging fruit" customer issues with current billing;
- Identify other (previously unidentified and "harder to fix") customer issues;
- Complete our analysis and report out of a previous billing review by Berry Dunn;
- Understand/identify process issues;
- Move us to the next step of process analysis to ensure the best tool and workflow

2 - Agile Project Management for Predictable Delivery

Agile	Waterfall
•75% Success rate •Resources are 25% more productive •Short delivery time means products to market faster •Takes weeks to plan •Lowers Risk •Issues are identified quickly •Very easy to make course corrections •Business is in full control of the delivery •Quality assurance is done from day one	•80% failure rate •Standish Group •Long delivery cycles -- expectations often not met •Takes months or years to plan •Increases Risk •Isolates Business from details of project •Difficult to make course corrections •Encourages Silos •Planning errors go undetected for months •Quality Assurance is an afterthought

"Agile Projects are 78% successful while traditional methods are less than 20% successful"
– The Standish Group

Agile development takes any project of any size and breaks it into many small, mini-projects, each lasting between two and four weeks. The agile approach is to deliver tested functionality every 3 – 4 weeks, versus 6 months to years for waterfall projects. Agile minimizes the risk, and improves the predictability be taking one large, high risk project and decomposing it into many small, lower risk projects.

Agile is a project management framework that maximizes the efficiently and quality of product delivery to end users.

- Requirements evolve but the timescale is *fixed*
- Capture requirements directly and visually from users for immediate development
- Develop small, incremental releases and iterate
- Focus on frequent delivery of products
- Complete each feature before moving on to the next
- Testing is integrated throughout the project lifecycle – test early and often
- A collaborative and cooperative approach between Agency and Technology

"Agile teams are 25% more productive then non agile developers"
– Scrum Alliance

To agencies, Agile gives the business control over what is delivered based on the priorities that are most valuable to the agency's mission. It also allows managers to know with very high accuracy how well the team is performing, not month to month but day by day:

- Lowers Risk: Problems are caught daily and fixed weekly, not in final testing when it's too late.
- Software works as business intends: business and IT are focused on same goal at the same time
- Reduced unexpected costs: initial quality is higher which mean less rework
- Develop direction changes with the business: priorities can change every three weeks.
- Agencies realize value faster: Finished pieces can be used as soon as they are completed

Maine is one of the leaders of public sector Agile project management

- Maine State Government has become practice leader: Already private sector companies have looked to the State of Maine to learn about our success with agile.

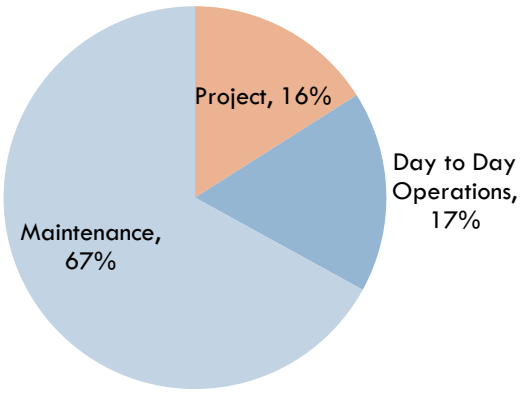
- Attract talent to state government careers: New IT graduates want to work for successful organizations – efforts like Agile and BPM help make the State of Maine an interesting place to work for new resources.

3 - Legacy Modernization – The Cost of the Past

Legacy Modernization is a process where applications, frequently very old, are replaced or significantly updated in order to realize substantial returns on investment. Legacy applications are more likely to break, and often use older, unsupported technology.

With legacy programs, the installed base of applications ironically becomes both more expensive and less relevant – because older applications are difficult to change, and they lock the agencies into older, inflexible workflow and processes.

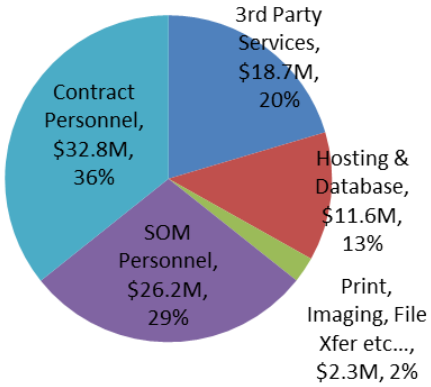
Operation and Project Metrics



84% of our operational expenses are allocated to maintenance and day to day operations

Currently, the State spends a disproportionate amount on legacy applications: 84% of our resources support older applications, while only 16% work on new development. While maintenance activities are unavoidable such a high maintenance burden is a strong indication of inefficiency.

State of Maine Application Costs



4 – Agency Needs and Technology Solutions

4.1 – Inventory of Agency Needs

Agency Need	Barriers	Agency	Solutions
Customer focused applications *One stop shopping*	• Increasingly mobile constituency • Silo-ed State processes • Data sharing	DHHS, DOL, DOT, DMR, IFW, DECD	• Ease of use • Context aware applications. • Geospatial services. • Application modernization • Advanced applications integration • Business Process Modernization

Improve Inter and Intra Agency data sharing.
 	
Interface technology and streamlined governance
	• Legacy systems
	• Archaic and diverse technology sets.
	• Inter-agency communications and governance
	• Inadequate flexibility in legacy file transfer solutions.
		All
		
		Specific interest: DHHS, DAFS, DOL
			• Standardize data sharing MOUs
			• Enterprise level data governance and awareness.
			• Agency/OPM/OIT Data User Group
			• Enterprise Services Bus
			  ○ Services oriented architecture that reduces or/and eliminates custom code.
			  ○ Insulates systems from changes to data partner systems.
			  ○ Marshal the use of redundant services

Data driven operations	• Legacy systems • Inter-agency communications and governance • Universal access to enterprise class tools	All Specific Interest: DAFS, DOT, DHHS, EDU, ACF, DOL	• Chief Data Officer • Data cleansing tools • Analytics and Report writing tools • Improved access to modern (Enterprise class) database technologies • Develop OIT KPIs
Increased application flexibility *This is particularly pressing for agencies subject to high regulatory and statutory volatility*	• Legacy systems • Archaic technology sets • Availability of Business SMEs	All Specific Interest: DEP, IFW, DMR, ACF, DHHS,	• Legacy modernization • AGILE development and support model • Customer enabled toolsets (Pega)
Serving a mobile workforce *Geographically dispersed workforce and mission obligations*		All Specific Interest: DOT, DEP, IFW, DMR, ACF, DPS, DHHS	Innovation area • Device independent applications ○ Responsive & Adaptive design • Geospatial services • Mobile Device Manager
Modernization of business processes and supporting systems	• Legacy applications • Aging workforce • Availability of Business SMEs	All	• Business Process Modernization • Legacy application modernization
Cost containment for commodity services *Storage, email, printing, imaging*	Reduced relevance of on premises solutions. High maintenance costs	All Specific Interest: DAFS, DEP, DMR, IFW, ACF, DOL, DOT	Cloud based solutions • Microsoft Office 365 – desktop software • OpenText – Content management
Securing data assets *Snowden proofing* *Intrusion protection*	Personally Identifiable Information HIPPA, DERPA, FTI, CJIS	All Specific Interest: DHHS, EDU, DAFS(OSC & MRS), DOL, DPS, DOC	• Encrypted Email • Encrypted workstations • Mobile Device Manager • Agency Cyber security training

Agency Need	Barriers	Agency	Solutions
Insulation of technology operations	• Legacy Applications • Aging infrastructure • Joint tenancy issues • Single points of failure	All Specific Interest: PUC, PFR, DOT, DHHS, DEP, ACF, IFW, DMR, MRS	• Cloud hosted applications. • Performance monitoring tools
Inter-agency application integration	• Institutional inertia • Legacy Applications	DECD, DPS, DMR, DAFS	• Advanced applications integration tools (ESB) • Cross domain governance
Business Continuity/Disaster Recovery		All Specific Interest: MRS, DOL, DHHS, DOT	Business impact analysis (BIA) leading to full implementation
OIT Financial Transparency – Billing and Project Execution		All Specific Interest: DOL, DEP, DPS, ACF	Estimation and cost tracking tools
Reliable Workforce	Silo-ed funding contributes to inflexibility of personnel assignments Work rules limit flexibility in performance management of staff	DEP, DMR, DPS, IFW, ACF	• Create service oriented technology provisioning units such a "Natural Resources & Licensing" or "Law Enforcement". Pool resources to limit risk. Share overhead. Combined concerted efforts • Internship program

4.2 – Agency Technology Tools – Bringing Efficiency to IT and Agency Operations

Tool	Description	Availability
Data correction and standardizing tools	Data correction tools have evolved to handle disparate data from different sources and using, business rules, have the ability to identify invalid data and make logical corrections. This could be used in legacy systems where data was not collected (all SSN's = 9) or is known to be incorrect (if family is receiving 'x' service from Agency they must be y. These rules and processes can be coded by agency resources; most do not require IT assistance.	Pilot
Business Intelligence and Data Analytics	Software that can analyze large or raw data sets to extract trends and predict future results	Live and Pilot. Some agencies, like DHHS and MRS, are already using third party software for forensic analysis, like fraud detection. With the start of the Agency – OIT Data analytics group, more 3rd party software options will be examined.
Business Process Management	Systematic approach to making an organizations workflow more efficient and transparent. Additional benefits: faster	Live in multiple agencies; Enterprise

	development and more end user capabilities (ability to change process)	agreement in place
Agile Methodology	Project development methodology that uses combined teams (business and IT) to produce testable results in short time frames (3 – 4 weeks). It keeps the request (end result) close to the process.	Live in multiple agencies; more work to be done. It requires a culture shift and trained resources
Enterprise Content Management	Document imaging and retrieval. Newer third party software is fast, efficient, has more capabilities, and is less expensive. It will allow SOM to replace existing paper based systems with digital imagining and processing.	2015 – Vendor has been selected (OpenText) and enterprise agreement will be signed.

Risk Management Tools

Cyber – Data Loss Prevention	DLP software detects if Personally Identifiable Information (PII – things like date of birth, SSN, etc) is being sent out of the organization thru oversight, carelessness, or malice. Over time, the tools are programmed by business resources to understand what is normal business and to flag exception cases.	MRS is actively working to install; other agencies are reviewing
Encrypted Email	Encryption of email so that only intended recipient can decrypt it. If the email is misdirected, the person receiving the email cannot read it. It is used where data such as data of birth, SSN, is sent so that an erroneous delivery does not give personal data to the wrong person. The agency can set the level of encryption.	OIT already supports this technology and it is covered in the rates. It is being used by ….
Encrypted Workstation (PCs, laptops)	This software encrypts information on a PC or laptop. If the laptop is lost or stolen, the information on it cannot be read.	OIT already supports this technology and it is covered in the rates. It is being piloted by some agencies.
Mobile Device Manager (MDM)	Enables remote wipe of data if smartphone is lost or stolen.	OIT already supports this technology and it is covered in the rates. It is being used by ….
Cyber Security Training	Technology is only one component of Cyber Security. The other two components are People and Process. Cyber Security training helps people avoid risky behavior, which includes everything from clicking on malicious email links to visiting sites know to have malware. Industry recommendations are that employees complete the training at list once a year.	OIT already supports this technology and it is covered in the rates. To date, thirteen agencies have completed training.

5 - Risk Management

5.1 - Cyber Security

The Office of Information Technology has made significant progress in the last three years in combating cyber threats. But Cyber Security threats continue to proliferate, and given a network of our size and complexity, the current Cyber Security posture is still not quite on par with industry best practices.

The Challenge

From a Cyber Security standpoint, The State Executive Branch network presents the following challenges:

- 400+ sites, stretching from Kittery to Madawaska
- 12,000 Users with desktops/laptops
- Approximately 1,000 Servers
- 30,000 "Other" Devices (Phones, Printers, Routers, HVAC Controllers, Cameras, etc.)
- 2,000 Applications
- Numerous non-state devices (approved and not approved)
- 1,000s of Remote Devices
- Commingled network with the Attorney General, Secretary of State, Audit, and the Judiciary, with no security walls in-between
- 20 Separate Lines of Business with different priorities
- External attacks have increased roughly five-fold in the last two years

Threat Metrics

On an average working day:

- 15 workstations get infected with malware, leading to loss-of-productivity of about six hours per workstation
- The firewall rebuffs some 5,000 intrusions
- 30,000 spam emails are blocked

Background

The citizens of Maine trust the State with a massive repository of personal information, including social security numbers, date of birth information, addresses. Breach of citizen personal information inflicts a stupendous damage to a government. At a minimum, it includes citizenry's loss-of-confidence in their government, statutory fines, the added expense of investigation and remediation, etc. Unfortunately, Cyber-attacks are becoming more common, and inflicting greater damages. Below is a partial list of state-level breaches in the last three-plus years. The most serious state-level breach was the South

Carolina Revenue breach of October 2012, which compromised 3.6M Social Security Numbers and 387,000 credit/debit cards. The cost of remediation has been estimated at $27M.

There are no guarantees in Cyber Security. In spite of best efforts, a network of our size and complexity will always have its weak points. But it is important to harden the network to industry best practices. This will dissuade hackers, who will then more likely move on to softer targets. Mitigating a Cyber Security breach post-fact is at least an order-of-magnitude more expensive than guarding against it.

Cyber Security is a matter of continuous vigilance, and is never fully done. OIT is proud of its accomplishments over the last three years. Nonetheless, the State still faces significant Cyber Security gaps.

5.2 - Business Continuity/Disaster Recovery

Background:

Business Continuity / Disaster Recovery (BC/DR) planning is how an organization guards against future disasters that could endanger its long-term health or the accomplishment of its primary mission(s). The ultimate goal is the recovery of an organization's critical functions and manpower after a disaster or major disruption.

Business Continuity is the overall recovery of a business after a major outage – a fire that prevents employees from entering the office, or a major chemical spill, or other incident. It could also be a major IT failure. It is what is needed to get employees functioning again.

Disaster Recovery is the recovery of critical IT systems after a major failure, such as cyber-attack, or failure in a data center, or major internet outage.

The need for deliberate planning, testing, and practicing of business continuity plans is increasing as our reliance on technology and greater exposure to risk from natural and man-made disasters increases. A new OIT BC/DR Program has been established to prepare an "all-hazards" approach to ensure the States technology infrastructure and procedures for continuing operations allows for normal or as near to normal productivity levels as possible.

Current State:

Currently, the State of Maine has several areas of 'single point of failure' where recovery from a major incident would take weeks or months. We have multiple data centers, but individually they could not support all

systems. Our storage, email, and networking systems all have lack the needed redundancy. Significant failure of any of these components could be catastrophic.

The OIT Business Continuity Program is transitioning from the "Program Initiation Phase" into the "Functional Requirements Phase" in Q1 of FY2015. A Business Impact Analysis Project is underway and will provide a comprehensive analysis of OIT as an organization; the outcome of the project will provide detailed information that provides a full understanding of prioritized mission-critical business functions, their required recovery time objectives, and their interdependencies. This information will be used to develop detailed Business Continuity Plans and select the optimum disaster recovery strategies in order to mitigate identified gaps.

Future State:

Once this BIA project is completed and the methodology refined, the process will be repeated (with assistance from OIT) throughout the enterprise so that both the agencies and OIT will have the most accurate picture of each business operating environment and ensure the best strategies and solutions are being implemented in the interest of protecting the State of Maine in the event of a disaster.

A key element of our disaster recovery capability is providing redundant infrastructure. A plan is being developed to prepare a backup data center that can provide redundancy for critical applications and services hosted in the primary data center. Additionally, available space will be on hand in the backup data center to recover and restore non-redundant applications and services in the event the primary data center is non-operational. As a supplement to this strategy, disaster recovery options within the cloud are being aggressively researched to determine suitability for our existing hosting environments and will be utilized where feasible over the next two years.

On-Going:

Regular testing and exercises are the key to a successful BC/DR program. OIT personnel with responsibilities within the BC/DR program will continue to receive required training appropriate to their roles within the plan. Quarterly table-top exercises are scheduled to be conducted at all levels within the BC/DR plan hierarchy with an annual operational exercise that will require team members to physically execute their assigned responsibilities.

The BC/DR program within OIT is projected to be fully implemented by the end of FY2015. Within 2 to 3 years, the program is projected to be fully mature and will be the example for other agencies within the enterprise to follow.

6 - Workforce Development

Workforce planning and development provides managers and supervisors with the tools to build a high performing workforce.

Workforce development is focused on recruiting, retaining, training, and succession planning.

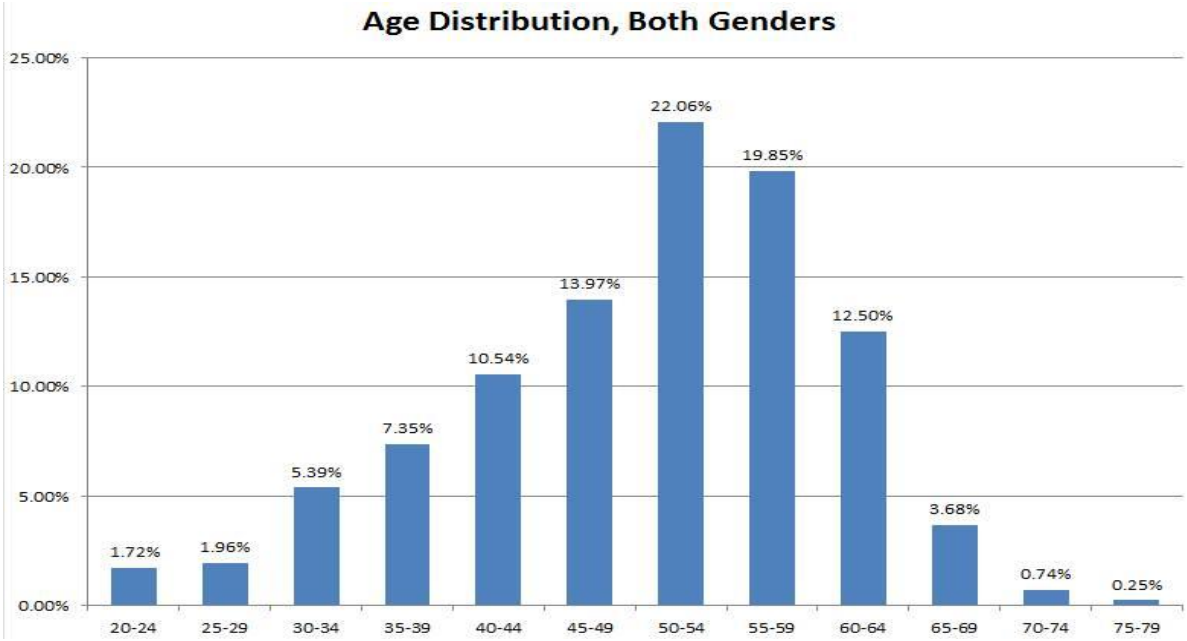
The challenges

Over 20% of the current OIT workforce will be able to retire in the next 2 - 3 years

There are **Four (4)** major trends—

- Aging government workforce
- Shrinking talent pool
- Meeting job expectations of younger generations
- Recognize a new set of skills in the public sector

Graph of Maine's Office of Information Technology's aging Workforce:



October 2014.

- Over the next 3 years we anticipate 86 employees, with over 1,600 years of State IT experience, will retire.

Need for New Skills- Talent Management

- Proficiency in project management
- Skills in mediation and negotiation
- Ability to collaborate across sectors and agencies
- Focus on contract management, risk analysis, and other complex skills.

The Current IT Workforce:

- Approximately 430 employees; 33 percent females; four employee bargaining units
- 70 different job descriptions and classifications
- Maintaining older technologies while embracing newer advanced technologies
- Subject to many regulations, legal constraints and labor contracts that impact workforce issues
- Four generations in the workplace –different need/expectations

Solutions -- Preparing for growing number of retirements and creating a pipeline to recruit talent

Interns

- This new OIT program has employed over 50 interns from local colleges in the last year
- Great feeder program – over 70% of our interns have become full time employees

Veterans hiring programs –

- Created partnerships with Veteran Outreach Career Centers and the National Guard to recruit talent from those returning from abroad, unemployed, or disabled, and re-entering workforce.
- Received the Patriot Award for outreach extended to an employee returning from abroad to the workplace.

Technology Night – We invite students from surrounding high schools to spend an evening with our IT professionals, learning about the career and opportunities since 2012. Survey results:

- 9% of the students who were not thinking of college replied they are now interested in college.
- Over 24% stated they were interested in pursuing an IT career as a result of Tech night.

Additional possible approaches:

Talent management – create a "pilot study" to utilize an assessment and talent management tool, such as *Caliper. Like private industry, use predictive testing to identify high potential employees.

Create An Intern Challenge:

Create a Governor's Intern Challenge to attract students who have interest and aptitude in information technology and cybersecurity. Interns, with an OIT mentor, will develop solutions for a business problem and then present to senior management.

Benchmark and partner with other State workforce leaders for "reusability" and work collaboratively to share ideas or program resources.

Use Technology, best practices and social media to improve efficiency and productivity in recruitment and onboarding

- LinkedIn reports 3/5 people use mobile to search for a job – need 1-click apply that works on any device – or they move on
- Use video and other media to tell our "fantastic" story – visual/audio

IT Infrastructure – Network, Servers, PCs, Telcom, Support

The History of OIT Infrastructure:

OIT was consolidated in 2005 to ensure consistent IT development, predictable project delivery, and to minimize risk. To consolidate, the individual pockets of IT were put under central management. But, this was only part of the need – there was not sufficient budget to build a robust, enterprise-level infrastructure and network. As such, many things were built for some term expediency rather than long-term foundation. We were challenged to keep our costs down, increase our services and meet the growing agency demands as well as unfunded mandates.

Current Environment

- **Infrastructure and User Equipment**:
  - Network – hundreds of State buildings and facilities (40,000+ devices connected)
  - Online citizen services (www.maine.gov) – accounts for some of this growth by handling 230 million contacts annually.
  - Remote access – average of 500-800 concurrent users during a typical business day (up to 1,200 users during a major snowstorm)
  - Wireless communications – 200 locations (480 access points)
  - Radio operations – 43 tower locations and 4,500 radios
  - Data centers – two major, two smaller
  - Servers – 679 Windows servers (296 virtual) + 190 Unix servers (33 virtual)
  - Storage – 393,000 gigabytes (393 terabytes)

- **User Equipment and Support:**
  - Telephone / voice services State-wide – over 15,000 phone extensions
  - IT customer support – 12,000 State employees
  - E-mail – 12,000 employees (46 million e-mails per year)
  - Desktop/ laptop computers – 3,000 built and issued per year
  - Blackberry and other mobile devices – over 2,500 users

Single Points of Failure in Network, Data Center and Storage

- Aging infrastructure in the Core Network.
- Incomplete fiber ring in the Augusta Metropolitan Network.
- Single access provider in the rural portions of the Wide Area Network.
- Augusta receives its primary Internet from the University of Maine at Orono. A secondary TimeWarner connection does exist from Portland, but its bandwidth is not comparable to that of the primary.
- Single point-of-failure of Email infrastructure.

- Even though the Oracle Database and the WebLogic middleware are clustered, they are not replicated across the two data centers, effectively making them single points-of-failure.
- The EMC storage is a single point-of-failure.
- The SQL Server database is a single point-of-failure.
- The various Windows (IIS) Application Servers are also single points-of-failure.
- The remote connection infrastructure is not sized to accommodate the State workforce.
- Network & Perimeter Security do not have adequate lab infrastructure. Which means, changes are routinely first implemented in production, resulting in indefensible business interruption.
- Commingled network among the Executive Branch, the Secretary of State, the Attorney General, and the Judiciary. An infected device in any of these Branches could spread the contagion to the entire network. And these four divisions are not subject to the same policy or oversight.

The Future Direction for OIT Infrastructure

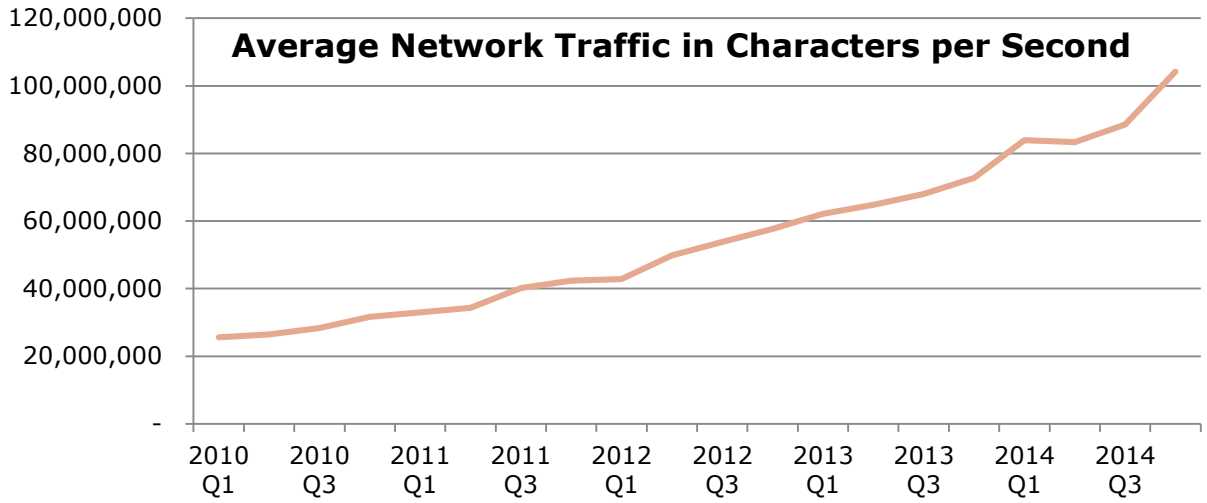
To support our agency needs and to minimize environment risk (cyber security, disaster recovery) we need to build a robust, flexible infrastructure. Over the course of the next five years the infrastructure must be built to meet the growing demands that will enable us to:

- Support a myriad of cloud service offerings (Office 365, Enterprise Content Management (ECM), Data Center, Virtualized Server Infrastructure, Interactive Voice Recognition (IVR), we also estimate a fair amount of agency Apps will also go to the cloud, etc.)
- Implement evolving hardware technology to manage the environment
- Allow us the growth within the infrastructure to modernize legacy applications
- Build redundant systems to prevent single points of failure

Network Reliability and Performance

In 2014 OIT contracted NTT Data for a 3rd party independent assessment of our network; based on those findings we are pursuing a redesign and modernization of the entire network. This will require an investment in hardware as well as contract staff to supplement OIT technicians in order to complete this initiative in a 12 – 24 month timeframe.

Over the past five years network traffic has increased 4-fold, handling 100 million bits (characters) per second. There are also approximately 230 million queries processed through web pages.

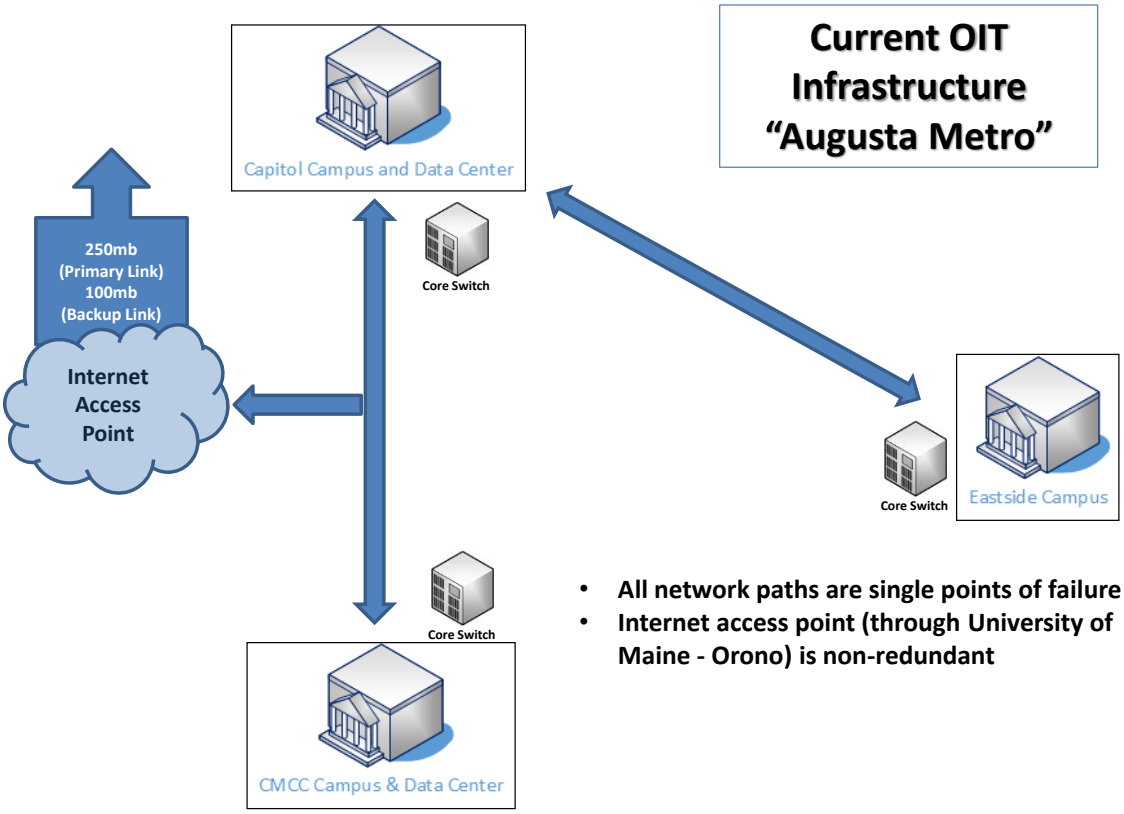


We currently process this information through two state owned and maintained data centers. We have limited redundancy between the data centers the current environment is not sufficient to sustain state government in the event of a catastrophic failure.

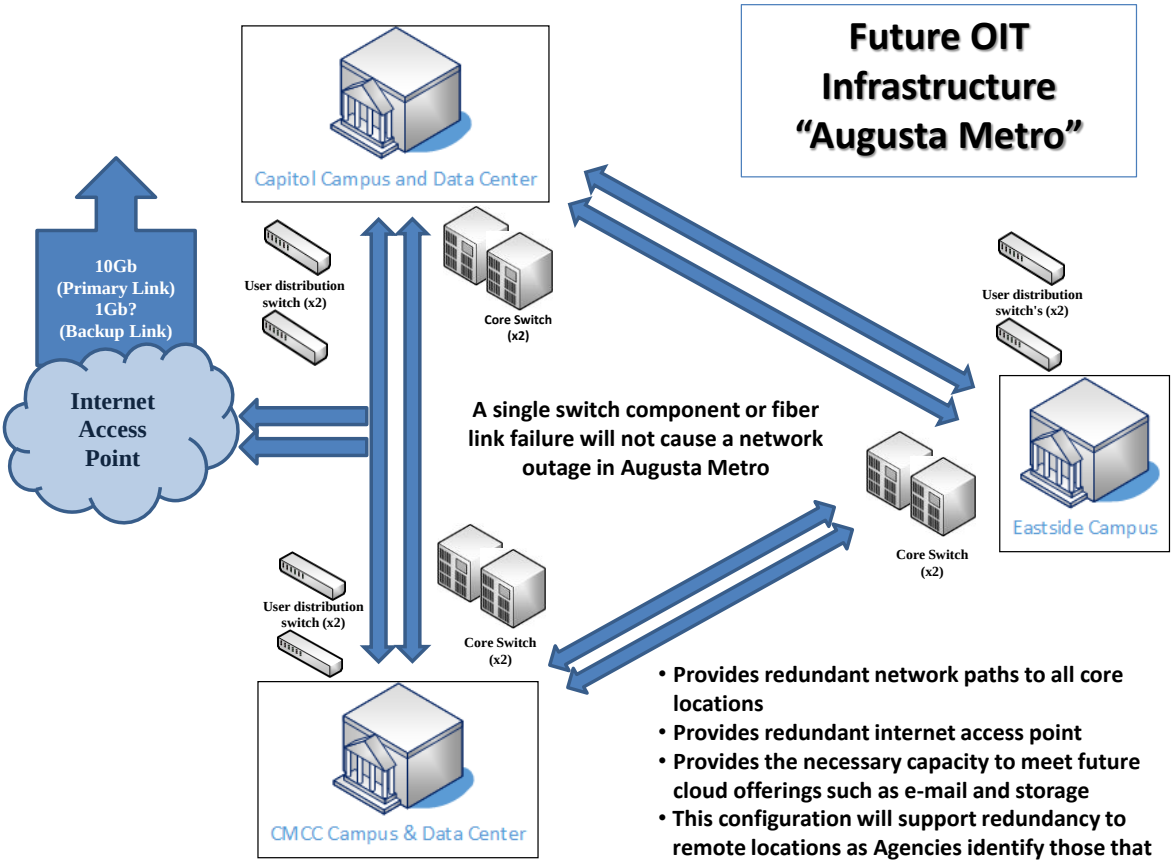
Building Redundancy into the Infrastructure

Redundancy of infrastructure is critical to ensure that agencies do not experience disruptions that may impact their ability to deliver services to their constituents. Disruptions can vary from a degradation of performance to outages for an extended period of time. IT Technology has developed a comprehensive plan to increase redundancy throughout all support areas.

Key components of this plan are a secondary data center and hosting environments. While applications and services such as storage can be located at either site, the infrastructure will be designed so that should a primary hosting site experience a problem, critical applications or services will failover to their secondary hosting environment with no interruption in service.



- All network paths are single points of failure
- Internet access point (through University of Maine - Orono) is non-redundant



A single switch component or fiber link failure will not cause a network outage in Augusta Metro

- Provides redundant network paths to all core locations
- Provides redundant internet access point
- Provides the necessary capacity to meet future cloud offerings such as e-mail and storage
- This configuration will support redundancy to remote locations as Agencies identify those that need it

National Recognition for the State of Maine

May 2014 **State Scoop 50 National Award "State Innovation of the Year" award for Business Process Management**

Maine's BPM program has been chosen as the winner of a StateScoop 50 Award for the category of State Innovation of the Year. Maine was recognized with a national "State Innovation of the Year" award for embracing an innovative and effective use of Business Process Management (BPM), leading to significant results for agency business partners.

June 2014 **Agile Government Transformation Award**

The State of Maine was recognized by Pega, our Business Process Management (BPM) vendor, as being a national leader in Business Process Management (BPM) and Agile Project Management. Agile Project Management allows for better project results, and has been proven to increase the efficiency and quality of projects managed with this discipline. Agile achieves greater effectiveness by utilizing: short release cycles, daily check-ins, greater customer involvement, and clear accurate reporting. Agile teams rely on close collaboration between business and technology experts that focus on clear deliverables.

From Jan 2014 **State Project Management Director 'Agile Delivery" Speaking Tour**

Maine's Director of Project Management has been invited to speak to groups across New England from both the public and private sector on how agile project management can lower risk and increase rewards projects and create high performing organizations.

From Jan 2015 **Technology and Strategic Planning Award**

The National Association of State CIOs (NASCIO) has chosen Maine as one of six states to highlight the use of technology and strategic planning. By aligning resources to match the Agile and BPM initiatives, Maine is better prepared for the future.

Appendix

Cyber Security Breach Details

State & Incident	Date Reported	Impact
West Virginia Email Virus Attack	Oct. 2014	6% of State computers taken down
Oregon Employment Database Breach	Oct. 2014	850,000 individual records, "some" including SSN
Colorado Finance & Accounting System Exposure	Sep. 2014	300 users have access to the Name, SSN, Bank Account Number, & Bank Routing Number of state vendors
Tennessee Employee Benefits Breach	Aug. 2014	60,000 employee health records
Montana Public Health & Human Services Server Breach	May 2014	1.3M of demographic records, including Name, Address, DOB, SSN
Maryland Developmental Disabilities Administration Case Management Breach	Mar. 2014	9,700 health records
South Carolina Employment & Workforce Breach	Jan. 2014	4,000 demographic records, including Name, DOB, SSN
Tennessee Treasury Breach	Dec. 2013	6,000 demographic records
Colorado I.T. Breach	Dec. 2013	19,000 demographic records, including Name, SSN
Florida Health Department Breach	Nov. 2013	3,500 demographic records, including Name, DOB, SSN
Vermont Health Exchange Breach	Nov. 2013	One user given access to another's demographic details, including Name, SSN, etc.

Florida Juvenile Justice Exposure	Jan. 2013	100,000 demographic records
South Carolina Revenue Breach	Oct. 2012	3.6M SSNs and 387,000 credit/debit cards. Impact to the state budget estimated at $27M.

State & Incident	**Date Reported**	**Impact**
Alaska Medicaid Exposure	Jun. 2012	Stolen USB Drive "possibly containing personally identifiable information." $1.7M fine.
California Child Support Exposure	Apr. 2012	800,000 demographic records, including Name, Address, DOB, & SSN
Texas Attorney General Exposure	Apr. 2012	6.5M unencrypted demographic records, including SSN
Utah Medicaid & Child Health Insurance Breach	Mar. 2012	280,000 SSNs and 500,000 "less-sensitive personal information". Total impact between $6M and $10M.
Texas Retirement & Unemployment Exposure	Mar. 2011	3.5M Name, Address, and SSN

Actions To-Date

OIT-Security has made immense strides over the last three years. Highlights include:

- Some 330,000 websites are blocked either because they contain inappropriate content or are known carriers of malware.
- The Governor's Cyber Security Executive Order (July 17, 2014) mandates annual Cyber Security Awareness Training for Executive Branch personnel. OIT is working with the various departments to roll it out.
- Deployment Certification ensures that any new information asset (be it an application or a server) going live is secure.
- OIT and MEMA have jointly launched the Cyber Security Incident Response Team, which focuses on creating capacity to respond to Cyber Security incidents.
- Two-Factor Authentication and Encrypted Tunnel are enforced for all remote connections to the State network.
- All OIT-managed devices have aggressive anti-malware.
- State email is subjected to aggressive spam filtration.

- Two Homeland Security devices monitor our external traffic and issues alerts for anomalies, vulnerabilities, etc.
- From time to time, OIT works with Homeland Security and other commercial entities for third-party security audits.
- OIT is currently rolling out Policy-based Email Encryption on a per-agency basis.
- OIT is in the process of rolling out File Volume Encryption, and Mobile Media (Thumb Drive, CDs, etc.) Encryption on a per-agency basis.
- OIT continues to meet with Senior Management Teams of Agencies that deal with a lot of personal information, such as DHHS, DOL, MRS, etc.

Gaps

In spite of considerable accomplishments over the three years, unfortunately, given the size and complexity of our network, there still exist vital gaps.

- Log Analysis: All devices (servers, routers, firewalls, etc.) generate voluminous logs. It is not humanly possible to peruse these logs, correlate them across devices, and derive meaningful information. The industry best practice is to outsource the log analysis to a managed service vendor. Unfortunately, that is currently not being done. Not analyzing logs deprives the State of trend-analysis of threats, and that leaves us vulnerable.
- OIT currently does not have any laboratory for the various Perimeter Security components (such as the Firewall, the Remote Virtual Private Network, the Domain Name Server, and the Dynamic Host Configuration Protocol). This inevitably means repairs and upgrades directly upon the production environment. Which, in turn, mean more risk and longer downtime.
- OIT currently does *not* have a functioning "Proxy Server." This is a piece of technology that hides the actual server on which an application runs when it advertises the URL. Right now, the URL of an application is an exact pointer to where the application actually lives. Thus, if the application contains personal information, hackers know exactly where to attack. A Proxy Server would enable divorcing the URL from its source, thereby offering a "separation wall". Acquiring and maintaining a Proxy Server would require about $100,000/annum.
- OIT's firewall resource bandwidth is far below customer demand, and this results in widespread dissatisfaction. OIT's firewall team currently consists of only two FTEs. Going by the statistics of existing unmet demand, OIT would like to add two more FTEs into the firewall team.
- Data Loss Prevention: This is an automated service that monitors for personal information templates (such as SSNs) on disks. Thus, if somebody downloads a hundred SSNs into a spreadsheet that lives in one of the monitored disks, this service will flag it. Further, it can be instructed to act in a number of ways: from just warning, all the way to preventing such a file from being written into the disk. This is a

must for any large organization dealing with personal information. Unfortunately, the State currently does not have this. MRS is willing to front the capital expenditure. But this will still require a fulltime FTE to maintain.

- Responding to the various security audits (Federal Social Security Administration, Federal Internal Revenue Service, Federal Affordable Care Act, State Department of Audit, etc.) is turning out to be a fulltime job. It is impossible to keep up with the current headcount. Not properly responding to audit leads to escalating penalties, up to and including, termination of Federal data flow. OIT would like to add one FTE for security audit response.
- The Executive Branch shares a commingled network with the Attorney General, Secretary of State, Audit, and the Judiciary, with no security walls in-between. The State network evolved over the last twenty-five years, when the dominant driver was cost. Thus, when the BMV office in Caribou had to be joined to the network, it was simply patched to the DHHS office in Caribou, because that was the least-cost wiring. However, the reality is that the Secretary of State maintains its own computer infrastructure. But if a Secretary of State's computer server were to be infected, that contagion could spread across the entire State network because there are no gates in the network. From a Cyber Security perspective, such an arrangement is less than optimal. Therefore, we must now add safeguards (gates) to segregate the various branches at the network layer. This does not involve capital expenditure, but requires additional resources. We estimate that the two additional firewall resources could be extended to accomplish this as a stretch goal.